PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-032244
(43)Date of publication of application : 31.01.2003

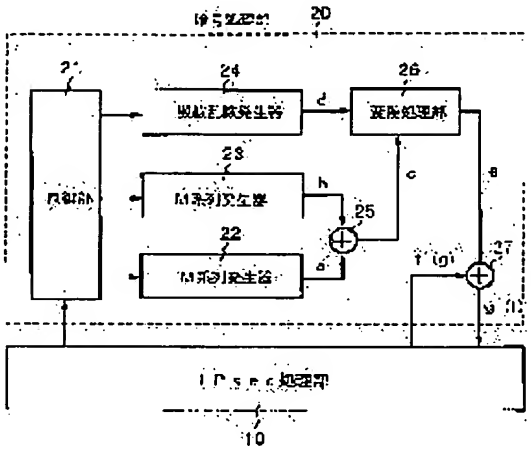
(51)Int.CI. H04L 9/24
G09C 1/00

(21)Application number : 2001-217546
(22)Date of filing : 18.07.2001

(71)Applicant : NEC CORP
(72)Inventor : SATO TSUTOMU

(54) STREAM CIPHER APPARATUS

(57)Abstract:
PROBLEM TO BE SOLVED: To solve the problem of communication with attached synchronization supervisory information or initial data in prior art lowering the transmission efficiency and also the cipher strength because of reused pseudo-random numbers.
SOLUTION: A pseudo-random number a generated by an M-sequence generator 22 is a repetitive sequence of pseudo-random numbers in a period of n bits. A pseudo-random number b, generated by an M-sequence generator 23, is a repetitive sequence of pseudo-random numbers in a period of m bits. An exclusive-OR gate 25 exclusive-ORs these pseudo-random members a, b bit by bit to generate one bit of pseudo-random number c. The sequence number of monotone increasing values by each enciphering of one IP packet is set in the generator 22 as initial data, fixed values are set in the generator 23 as initial data, so that the pseudo-random numbers used for enciphering one IP packet always use a different partial sequence of the pseudo-random numbers c. Enciphering or decoding is conducted, using pseudo-random numbers e generated from the pseudo-random numbers c and pseudo-random numbers d.



LEGAL STATUS

[Date of request for examination] 12.06.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]